AZMI & ASSOCIATES
A member of TerraLex worldwide | advocates & solicitors

Part 1: Introduction

In Malaysia, collection, processing, storage, transfer and retention of individuals' personal data are governed under the Personal Data Protection Act 2010 (the "**Act**"). In short, the Act regulates the processing of personal data in commercial transactions in Malaysia.

In 2019, the Personal Data Protection Commissioner Malaysia ("**PDPCM**") has undertaken the Act's compliance inspections on business and commercial entities operating in Malaysia as the follows:

No.	Sectors	Number of Inspections
1.	Pawnbroking	3
2.	Money Lending	1
3.	Utilities (Water)	1
4.	Services	6
5.	Transportation (Air)	0
6.	Education	1
7.	Tourism and Hospitalities	5
8.	Health	2
9.	Direct Sales	0
10.	Insurance	2
11.	Banking Industry and Financial Institutions	2

Personal Data System Inspection on the Data User for 2019.[1]

It is therefore apparent that PDPCM's enforcement approach in year 2019 had focused on the sectors of services, education, tourism and hospitalities, in particular the services sector, where the number of inspection visits conducted by PDPCM was approximately twenty (20) % of the total conducted inspections.[2]

Part 2: Six (6) Things You Need to Know on Personal Data Protection

1. Is Your Business Required to Comply with the Act?

As mentioned above, any processing of personal data in the context of commercial transactions would inevitably attract the application of the Act. Under the Act, "commercial transactions" include any matters relating to:

(i) the supply or exchange of goods or services;

(ii) agency;

(iii) investments;

(iv) financing;

(v) banking; and

(vi) insurance.[3]

Nevertheless, it is imperative to also note that the Act does not apply to:

(a) Federal Government and State Governments;[4]

(b) where personal data are being processed outside of Malaysia, unless it is intended to be further processed in Malaysia;[5] and

(c) credit report agencies under the Malaysia Credit Reporting Agencies Act 2010.[6]

2. Does Your Business Involve Processing of Personal Data?

Under the Act, the term "processing" refers to the collecting, recording, holding or storing of the personal data or carrying out any operation or set of operations on the personal data. For ease of understanding, below are some of the examples which may be considered as processing:

(i) Collecting data through forms, by phone or via the web;

(ii) Publishing data;

(iii) Selling data;

(iv) Using administrative data;

(v) Using data for marketing purposes;

(vi) Recording data;

(vii) Disclosing or providing data to other organizations; and/or

(viii) Destroying data.[7]

3. Is Your Business Complying with the Personal Data Protection Principles?

In essence, the application of the Act revolves around seven (7) fundamental principles, namely[8]:

(i) the General Principle;

(ii) the Notice and Choice Principle;

(iii) the Disclosure Principle;

(iv) the Security Principle;

(v) the Retention Principle;

(vi) the Data Integrity Principle; and

(vii) the Access Principle.

Under the Act, failure to comply with any of the seven (7) principles will attract a fine not exceeding RM300,000.00 or imprisonment not exceeding two years or to both.[9]

4. Are There Any Guidelines or Standards Issued on the Compliance of the Seven (7) Principles?

According to the PDPCM, the principles which are commonly breached by entities are the general, security, retention, and disclosure principles. This was probably caused by the concerns of having to bear the costs of compliance with the principles especially for the SME's owners. In addition, the lack of awareness of the public or businesses towards the personal data protection in our country also contributed to the breaches.[10]

Premised on such, the Personal Data Protection Standard 2015 ("**Standard 2015**") was introduced whereby it established the following three (3) minimum mandatory principles which entities must strictly adhere to:

(i) the Security Principle;

(ii) the Retention Principle; and

(iii) the Data Integrity Principle.

The penalty for non-compliance of such minimum mandatory principles, upon conviction, will attract a fine not exceeding RM250,000.00 or imprisonment not exceeding two years or to both.[11]

Nonetheless, it is still compulsory to comply with the other remaining principles of the seven (7) fundamental data protection principles as mentioned above. This is because the penalties are not mutually exclusive. Therefore, if a commercial organisation has failed to comply with both

(i) the requirements under the Standard 2015; and

(ii) the principles under the Act,

it and/or its officers will be liable for penalties and/or imprisonment under both.

5. What Are The Minimum Standards Under the Security Principle, the Retention Principle and the Data Integrity Principle?

The PDPCM has provided the following minimum standards to assist data users and processors to comply with the Security Principle, the Retention Principle and the Data Integrity Principle:

(a) Security Principle

In processing a data subject's personal data, a data user or processor is required to undertake all reasonable and practicable steps preventing any loss, misuse, modifications, unauthorized or accidental access or disclosure, alteration or destruction of the said data.[12] On the other hand, where the data processing is carried out by an external third party, it is imperative to note that the data user must secure a sufficient guarantee from the third party service provider in respect of its security measures for the protection of the data and to undertake all reasonable steps to ensure compliance of this principle.[13]

(b) Retention Principle

This principle stipulates that a data subject's personal data must not be retained longer than necessary for the fulfilment of the purpose for which it is being processed.[14] Upon fulfilment of the said purpose, it is the duty of the data user to take all reasonable steps to destroy or permanently delete all personal data after the retention period.[15] The retention periods are varied in accordance to the requirements set out by different laws, for instance data regarding employee payrolls is required to be kept for seven (7) years long.[16] On the other hand, if the data does not hold any legal value, it shall be disposed of within 14 days, whilst inactive personal data shall be disposed of within 24 months.[17]

(c) Data Integrity Principle

This principle imposes a continuous obligation upon data users to take reasonable steps to ensure that the personal data to be accurate, complete, not misleading and kept up-to-date by having regard to the purpose, for which the personal data was collected and further processed.[18]

The above are some of the minimum standards that the PDPCM has prescribed to assist data users and businesses in working towards compliance with the above-mentioned three (3) data principles which are commonly breached. It is still mandatory to comply with the remaining principles of the seven (7) data principles as prescribed by the Act.

6. Some Steps That Your Business Can Take To Ensure Compliance with the Minimum Standards

The following are some of the steps that your business may take to meet the minimum standards of data protection:

(a) Security Principle

DO's	DON'Ts
• Access control is well-established and safeguarded. • ID and Password management is well-established, maintained and secured. • Documents are kept at secure locations/databases.	• Documents containing personal data are placed at inappropriate, or unsecured or publicly accessed locations • Documents are exposed and not properly kept and retained. • Malfunctioned CCTV and delays in remedying the same resulting in further data or financial losses. • Documents are not properly disposed or destroyed. • Passwords to computer log in system are exposed and shared with colleagues.[19]

(b) Retention Principle

DO's	DON'Ts
• All documents containing personal data are stored at secure location. • An effective procedure of unused record and data disposal is well established and adhered to.	• Improper storage of business contracts, customers and suppliers data and financial records or documents. • Improper or careless use of storage cabinets or facilities. • Lack of effective policy on data retention & disposal. • Cabinets used to store items other than documents.[20]

(c) Data Integrity Principle

DO's	DON'Ts
• To prepare a form for data subjects to update personal data online or via a physical copy; • To update, correct or amend personal data immediately upon receiving a personal data correction notice from the data subjects; • To ensure that all relevant legislation requirements are fulfilled by identifying the types of data or documents that are required to support or verify the authenticity of the personal data of the data subjects; and • To inform the data subjects about the procedure and ways of updating of their personal data either through an on-line portal or by displaying an announcement or notice on the data user's premises, and by other appropriate methods of notification or alertness.	• Possession or retention of obsolete or misleading personal data; • Data is tampered by hackers or anonymous scammers; • The updated and uploaded information is false or inaccurate.[21]

Part 3: Conclusion

The perpetual advancement of information technology in this era has undoubtedly come with a price as digital theft, fraud and hacking activities continue to cause anxieties, discomforts and losses among data subjects. As reiterated by the CEO of CyberSecurity Malaysia, Datuk Dr Amirudin Abdul Wahab, heavier penalties for data breach offenders are being discussed to ensure data subjects' personal data are always safeguarded.[22]

SME's owners are urged to comply with the above data protection standards and principles despite facing potentially high compliance costs. All in all, regardless of the existence and application of the minimum standards, it is mandatory for the data users or any companies processing personal data to abide with the seven (7) principles stipulated under the Act. Any enterprise that has concerns as to whether its business operation including data processing and retention are in compliance with principles of the Act and the minimum standards as discussed above is advised to seek legal advice accordingly.

---

1 Annual Report of Personal Data Protection Commissioner Malaysia 2019
2 ibid.
3 Section 2 of the Act
4 Section 3 (1) of the Act
5 Section 3 (2) of the Act
6 Section 4 of the Act
7 https://www.pdp.gov.my/jpdpv2/frequently-asked-questions/?lang=en
8 Section 5 of the Act
9 https://www.pdp.gov.my/jpdpv2/assets/2020/01/PDPA-Implementation-in-Organisation.pdf
10 Regulation 12 of Personal Data Protection Regulations 2013
11 Section 5(2) of the Act
12 Section 9(1) of the Act
13 Section 9(2) of the Act
14 Section 10(1) of the Act
15 Section 10(2) of the Act
16 Section 82 of Income Tax 1967
17 Paragraph 6 of Standard 2015
18 Section 11 of the Act
19 https://www.pdp.gov.my/jpdpv2/assets/2019/09/PDPA-Compliance-Jan-2019.pdf
20 Ibid.
21 Ibid.
22 https://themalaysianreserve.com/2019/10/21/heavier-fines-for-hackers-hasty-data-holding-firms/

Prepared by:

Lee Kin Hing
Senior Associate 1
leekinhing@azmilaw.com

Ong Sern Tai
Associate
ongserntai@azmilaw.com

Chris Lim Chee Kiung
Trainee Solicitor
chrislim@azmilaw.com

Corporate Communications
Azmi & Associates

05 March 2021